

REMARKS

Claims 1 to 20 were pending in the application at the time of examination. Claims 1, 3-4, 6-17 and 19 stand rejected as anticipated. Claims 2, 5, 18, and 20 stand rejected as obvious.

Claims 1, 12, and 17 have been amended. Applicant submits support for the amendments can be found in the specification at least at: FIG. 6; page 16, line 24 through page 23, line 26; and page 14, lines 18-23. Claims 1-20 are pending in the application.

Rejections under 35 U.S.C. 102(e)

In reference to rejections under 35 U.S.C. §102(e), the MPEP 2131 states in part:

TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Claims 12-16 are patentable over Khazan (US Pub. No. 20050108562 A1).

In the Office Action at page 2, paragraph 2, the Examiner states:

...Khazan discloses (fig. 4A; [0040]) shows a malicious code detection device (110) including: an intercept module (114; [0073]); an analyzer module (104-108; [0076]) coupled to the intercept module (114); a request database (see figs. 1, 4A) coupled to the analyzer module (114; [0032]); and a standards list (106) coupled to the analyzer module (108; see [0040][0072; 0078].

Applicant respectfully traverses the Examiner's rejections.

Applicant's Claim 12 recites in part:

an intercept module, the intercept module for intercepting a request issuing on a host computer system prior to the sending of the request from the host computer system to a target computer system;

an analyzer module coupled to the intercept module;

a request database coupled to the analyzer module, the request database including one or more request entries, **each of the one or more request entries identifying a request determined to be suspicious;** and

a standards list coupled to the analyzer module, the **standards list including selected standards for use in determining whether the request is suspicious.** (emphasis added)

The reference to Khazan at [0032] relied on by the Examiner describes:

(e)ach of the host computer systems may perform different types of data operations in accordance with different types of tasks. In the embodiment of FIG. 1, any one of the host computers 14a-14n may issue a data request to the data storage system 12 to perform a data operation, such as a read or a write operation.

Applicant submits that the mere issuance of a data request from host computers 14a-14n to data storage system 12 does not teach or suggest at least a "request database including one or more request entries, each of the one or more request entries **identifying a request determined to be suspicious**" as recited in part in Applicant's Claim 12 (emphasis added). Further the ability of data storage system 12 to perform a data operation such as a read or a write also does not teach or suggest at least a "request database including one or more request entries, each of the one or more request entries **identifying a**

request determined to be suspicious" as recited in part in Applicant's Claim 12 (emphasis added).

With regard to the Examiner's references to Khazan at [0072] and [0078], Applicant fails to appreciate any reference to a structure which teaches or suggests a "standards list including selected standards for use in determining whether the request is suspicious" as recited in part in Applicant's Claim 12. If the Examiner maintains this rejection, the Examiner is respectfully requested to identify with specificity a structure in paragraphs [0072] and [0078] that the Examiner views as teaching or suggesting the "standards list" of Claim 12.

The reference to Khazan at [0040] relied on by the Examiner describes in part:

Referring now to FIG. 4A, shown is an example of an embodiment of components that may reside and be executed on one or more of the host computer systems included in the computer system 10 of FIG. 1. The components 100 in this embodiment include...the list of targets and invocation locations 106...

Applicant submits the above citation to Khazan merely describes a list 106 including **locations**, i.e., target and invocation locations, and does not teach or suggest at least "the standards list including **selected standards for use in determining whether the request is suspicious**" as recited in part Applicant's Claim 12 (emphasis added). Indeed, Khazan at [0067] describes the location pairs of list 106 as characterizing "normal behavior" of an executing application, and not suspicious behavior.

For the above reasons, Applicant submits the references to Khazan relied on by the Examiner fail to anticipate Claim 12, and that Claim 12 is patentable over Khazan.

Claims 13-16 depend from Claim 12 and therefore include at least the limitations of Claim 12. Thus, for at least the same reasons presented above with regard to the rejection of Claim

12, hereby incorporated by reference, Claims 13-16 are also not anticipated by and are patentable over Khazan.

Applicant respectfully requests reconsideration and withdrawal of the rejections of Claim 12-16.

Claims 1 and 17 are patentable over Khazan (US Pub. No. 20050108562 A1).

In the Office Action at pages 2-3, paragraph 2, the Examiner states:

...Khazan (figs. 1, 4A) discloses a method including stalling a request (fig. 1 shows a data storage system 12 for holding a request; see [0032]; and determining whether the request is suspicious, wherein upon a determination that the request is suspicious, determining whether malicious code activity is detected based upon the request ([00120])).

Applicant respectfully traverses the Examiner's rejections.

Applicant's Claim 1 recites in part:

stalling a request on a host computer system prior to sending the request to a target computer system;

determining whether the request is suspicious; wherein upon a determination that the request is not suspicious, releasing the request; and

wherein upon a determination that the request is suspicious, adding a request entry to a request database, the request entry identifying the request, **generating a counter value associated with the request entry,**

determining whether the counter value meets a counter value threshold, and

wherein upon a determination that the counter value meets the counter value threshold, determining that malicious code activity is detected. (emphasis added).

Initially, Applicant wishes to point out to the Examiner that the reference to Khazan at [00120] is not present in the published application. The last numbered paragraph in the referenced application is [0119]. Thus Applicant cannot effectively address the Examiner's reference. If the Examiner maintains this rejection, the Examiner is respectfully requested to identify with specificity the particular paragraph in Khazan relied on by the Examiner.

However, Applicant submits that Khazan does not teach or suggest at least **"generating a counter value associated with the request entry", "determining whether the counter value meets a counter value threshold", or "wherein upon a determination that the counter value meets the counter value threshold, determining that malicious code activity is detected"** as recited in part in Applicant's Claim 1 (emphasis added).

For the above reasons, Applicant submits the references to Khazan relied on by the Examiner fail to anticipate Claim 1 and that Claim 1 is patentable over Khazan.

As Claim 17 similarly recites the above limitation of Claim 1, Applicant submits that for at least the same reasons presented above with regard to the rejection of Claim 1, Claim 17 is not anticipated by and is patentable over Khazan.

Applicant respectfully requests reconsideration and withdrawal of the rejections of Claims 1 and 17.

Claims 3, 4, 6-11 and 19 are patentable over Khazan (US Pub. No. 20050108562 A1).

In the Office Action at page 3, paragraph 2, the Examiner states:

...the claims differ from claim 1 by the additional limitations "wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request

database, and determining whether malicious code activity is detected on the host computer system based upon the request entry." However, the limitations are clearly disclosed by Khazan (fig. 11; [0102-0103]).

Applicant respectfully traverses the Examiner's rejections.

Applicant's Claim 3 recites in part:

intercepting a request on a host computer system;
stalling the request; and
determining whether the request is suspicious,
wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database, and
determining whether malicious code activity is detected on the host computer system based upon the request entry. (emphasis added).

The reference to Khazan at [0102] relied on by the Examiner describes:

Referring now to FIG. 10, shown is an example of one embodiment of a data structure that may be used to store the target location and corresponding invocation location pairs 106. In this embodiment, the structure 500 includes an array of target locations. Each target location has an associated linked list of associated invocation locations. Since each target location may be invoked zero or more times, the associated linked list may have zero or more entries. The target locations maybe stored in a sorted order, such as, for example, in sorted order based on symbol name of the associated API or target routine.

And, the reference to Khazan at [0103] relied on by the Examiner describes:

Referring now to FIG. 11, shown is an example of another embodiment of a data structure that may be used to store the target location and corresponding

invocation location pairs 106. In this embodiment, the structure 550 includes a linked list of entries in which each entry corresponds to one of the target location and corresponding invocation location pairs. The entries may be stored in a sorted order, such as in order of increasing invocation location is each programming or code segment.

Applicant submits the above references to Khazan relied on by the Examiner merely describe two examples of data structures that may be used to store the target location and corresponding invocation location pairs 106. Khazan does not describe that a determination as suspicious is needed in order for location pairs to be entered in list 106. Indeed Khazan at [0067] describes the location pairs of list 106 characterize "normal behavior" of an executing application. When deviations from the predetermined location pairs of list 106 are detected during later execution of an application, a determination can then be made that an application includes malicious code (Khazan [0067]). Thus, as the location pairs in list 106 characterize "normal behavior" and are not determined to be suspicious in order to be added to list 106, the references to Khazan relied on by the Examiner do not teach or suggest at least **"wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database"** as recited in part in Applicant's Claim 3 (emphasis added).

For the above reasons, Applicant submits the references to Khazan relied on by the Examiner fail to anticipate Claim 3 and that Claim 3 is patentable over Khazan.

As Claims 4 and 6-11 depend from Claim 3 and therefore include at least the limitations of Claim 3. Thus, for at least the same reasons presented above with regard to the rejection of Claim 3, hereby incorporated by reference, Claims 4 and 6-11 are also not anticipated by and are patentable over Khazan.

As Claim 19 similarly recites the above limitations of Claim 3, Applicant submits that for at least the same reasons presented above with regard to the rejection of Claim 3, Claim 19 is not anticipated by and is patentable over Khazan.

Applicant respectfully requests reconsideration and withdrawal of the rejections of Claims 3, 4, 6-11, and 19.

Rejections under 35 U.S.C. 103(a)

Claims 2 and 18 are patentable over Khazan (US Pub. No. 20050108562 A1) in view of Bates (USPN 6,785,732).

In the Office Action at page 4, paragraph 4, the Examiner states:

...Khazan does not explicitly disclose a method, which generates a notification that malicious code activity is detected; and implements one or more protective actions.

However, in the same field of endeavor, Bates discloses a computer system including a virus checker, which generates a notification that malicious code activity is detected; and implements one or more protective actions (col. 6, lines 21-38).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to combine Khazan's malicious code detection technique with the virus checker system, as disclosed by Bates. By doing so, senders of viruses are notified when a web server detects a virus, thus helping to inhibit the proliferation of the virus (col. 2, lines 51-56).

Applicant respectfully traverses the Examiner's rejections.

Claim 2 depends from Claim 1, and additionally cites in part the limitation of:

...generating a notification that malicious code activity is detected.

As earlier discussed with regard to the rejection of Claim 1 under 35 U.S.C. 102(e), the references to Khazan relied on by the Examiner fail to teach or suggest at least "generating a counter value associated with the request entry", "determining whether the counter value meets a counter value threshold", or "wherein upon a determination that the counter value meets the counter value threshold, determining that malicious code activity is detected" as recited in part in Applicant's Claim 1.

The cited references to Bates do not cure this deficiency in Khazan. Thus, the combination of Khazan in view of Bates does not teach or suggest at least "generating a counter value associated with the request entry", "determining whether the counter value meets a counter value threshold", or "wherein upon a determination that the counter value meets the counter value threshold, determining that malicious code activity is detected" as recited in part in Applicant's Claim 1. Accordingly, Claim 1 is not obvious in view of and is allowable over the combination of Khazan in view of Bates.

Claim 2 depends from Claim 1 and therefore includes at least the limitations of Claim 1. Thus, for at least the same reasons presented above with regard to Claim 1, hereby incorporated by reference, Claim 2 is also not obvious in view of and is patentable over the combination of Khazan in view of Bates.

As Claim 17 similarly recites the above limitations of Claim 1, and Claim 18 depends from Claim 17, Applicant submits that for at least the same reasons presented above with regard to the rejection of Claim 2, Claim 18 is not obvious in view of and is patentable over Khazan in view of Bates.

Applicant respectfully requests reconsideration and withdrawal of the rejections of Claims 2 and 18.

Claims 5 and 20 are patentable over Khazan (US Pub. No. 20050108562 A1) in view of Bates (USPN 6,785,732).

Claim 5 depends from Claim 3, and additionally cites in part the limitation of:

...generating a notification that malicious code activity is detected on the host computer system.

As earlier discussed with regard to the rejection of Claim 3 under 35 U.S.C. 102(e), the references to Khazan relied on by the Examiner fail to teach or suggest at least "wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database" as recited in part in Applicant's Claim 3.

The cited references to Bates do not cure this deficiency in Khazan. Thus, the combination of Khazan in view of Bates does not teach or suggest at least "wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database" as recited in part in Applicant's Claim 3. Accordingly, Claim 3 is not obvious in view of and is allowable over the combination of Khazan in view of Bates.

Claim 5 depends from Claim 3 and therefore includes at least the limitations of Claim 3. Thus, for at least the same reasons presented above with regard to Claim 3, hereby incorporated by reference, Claim 5 is also not obvious in view of and is patentable over the combination of Khazan in view of Bates.

As Claim 19 similarly recites the above limitations of Claim 3, and Claim 20 depends from Claim 19, Applicant submits that for at least the same reasons presented above with regard to the rejection of Claim 5, Claim 20 is not obvious in view of and is patentable over Khazan in view of Bates.

Applicant respectfully requests reconsideration and withdrawal of the rejections of Claims 5 and 20.

Appl. No. 10/633,907

Amdt. dated February 16, 2006

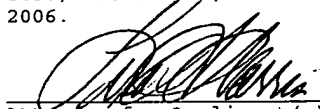
Reply to Office Action of November 17, 2005

Conclusion

For the foregoing reasons, Applicant respectfully requests allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on February 16, 2006.


Attorney for Applicant(s)

February 16, 2006
Date of Signature

Respectfully submitted,



Lisa A. Norris
Attorney for Applicant(s)
Reg. No. 44,976
Tel.: (831) 655-0880